WE CLAIM:

1. A computer-readable medium having computer-executable instructions for protecting domain data against unauthorized modification, comprising:

receiving at a first computing machine a request to modify an object associated with a shared data structure, the shared data structure spanning a plurality of domains, the object including a security descriptor identifying an owner domain in the plurality of domains;

determining whether the first computing machine is within the owner domain; and

if the first computing machine is not within the owner domain, rejecting the request to modify the object.

2. The computer-readable medium of claim 1, further comprising, if the first computing machine is within the owner domain, allowing the request to modify the object.

3. The computer-readable medium of claim 1, wherein the shared data structure includes at least one data store that is replicated among each of the plurality of domains, and wherein the object is contained within the replicated data store.

4. The computer-readable medium of claim 1, wherein determining whether the first computing machine is within the owner domain comprises retrieving from the security descriptor the identity of the owner domain and comparing the owner domain identity to the domain within which the first computing machine resides.

5. The computer-readable medium of claim 1, wherein the security descriptor further comprises a field that indicates whether a special security evaluation should be performed on requests to modify the object, and wherein the computer-executable instructions further comprise, if the field indicates that the special security

evaluation should be performed, causing the special security evaluation to be performed.

6. The computer-readable medium of claim 5, wherein the special security evaluation comprises causing requesting that a second computing machine within the owner domain evaluate whether an entity issuing the request to modify the object is authorized to modify the object.

7. A computer-implemented method for protecting domain data against unauthorized modification, comprising:

receiving from a requester at a first machine in a first domain in a plurality of domains a request to modify an object, the request including a security token identifying at least one group of which the requester is a member, the object having an associated security descriptor identifying an owner domain for the object, the object having a flag to identify whether a special security evaluation is to be performed on requests to modify the object;

determining from the flag whether the special security evaluation is to be performed on the request to modify the object;

if the flag indicates in the affirmative, then performing the special security evaluation on the request to modify the object; and

if the special security evaluation approves the request to modify the object then allowing the request to modify the object to proceed.

8. The computer-readable medium of claim 7, wherein the special security evaluation comprises passing the security token associated with the request and the security descriptor associated with the object to the owner domain for evaluation.

9. The computer-readable medium of claim 7, further comprising, if the flag indicates in the negative, then performing a security evaluation on the request to modify the object.

10. The computer-readable medium of claim 9, wherein the security evaluation comprises comparing the security token with the security descriptor to determine whether the requester is a member of any groups that have been granted permission to access the object.

11. The computer-readable medium of claim 10, wherein the security evaluation further comprises determining whether the request to modify the object is a modification for which the requester is privileged on the first machine regardless of whether the requester is a member of any groups that have been granted permission to access the object.

12. The computer-readable medium of claim 11, wherein the security evaluation further comprises if the requester is privileged to perform the request to modify the object, and the requested modification is a fundamental modification of the object, then denying the request if the first domain is not the owner domain for the object.

13. A computer-readable medium having computer-executable components to protect domain data against unauthorized modification; comprising:

a shared data structure that spans a plurality of domains, at least two domains in the plurality of domains having a transitive trust relationship wherein a user authentication within one of the two domains is honored in the other of the two domains, the shared data structure having at least one data store that is replicated among each of the plurality of domains;

an object stored within the data store, the object having a plurality of attributes, at least one of the attributes being related to security access rights associated with the object, the security access rights including an owner domain identifier identifying one of the domains within the plurality of domains; and

a security system configured to receive a request to modify the object; to retrieve from the object the owner domain identifier, to compare the owner domain identifier with an identifier of a domain from which the request originated, and to reject

the request to modify the object if the owner domain identifier does not match the identifier of the domain from which the request originated.

14. The computer-readable medium of claim 13, wherein:

the security access rights associated with the object further comprise an indicator that an attempt to access the object is to be evaluated within the domain identified by the owner domain; and

the security system is further configured to, prior to performing a security evaluation on a received request to modify the object, determine from the indicator whether the request to modify the object should be evaluated within the domain identified by the owner domain, and if so, to return a notification to the requestor that the security evaluation is to be evaluated within the domain identified by the owner domain.

15. The computer-readable medium of claim 14, wherein the notification to the requestor comprises a referral message including an identification of the owner domain.

16. The computer-readable medium of claim 13, wherein the security system if further configured to determine whether the request to modify the object originated within a particular domain of the plurality of domains, and if so, then to perform a standard security evaluation of the request to modify the object without resort to the owner domain.

17. The computer-readable medium of claim 16, wherein the particular domain is a root domain of the shared data structure.

18. The computer-readable medium of claim 13, wherein the shared data structure comprises a directory service and wherein the at least one data store comprises configuration data associated with the directory service.

19. The computer-readable medium of claim 13, wherein the shared data structure comprises a directory service and wherein the at least one data store comprises schema data associated with the directory service.

20. The computer-readable medium of claim 13, wherein the at least one attribute comprises a security descriptor, and the owner domain identifier is part of an owner security identifier.